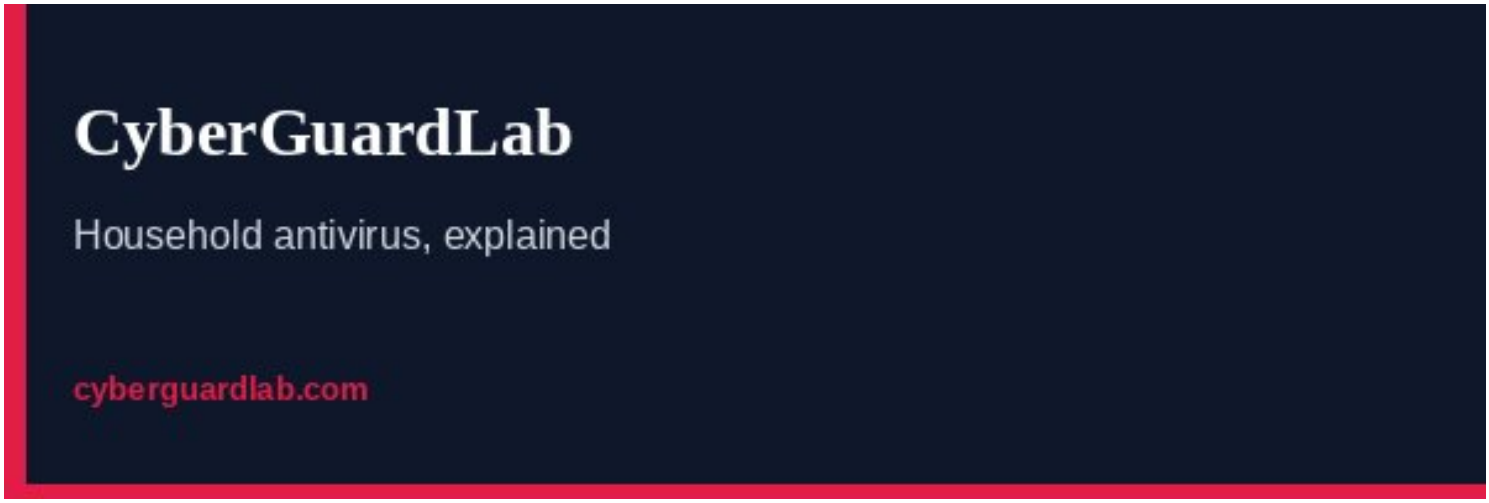
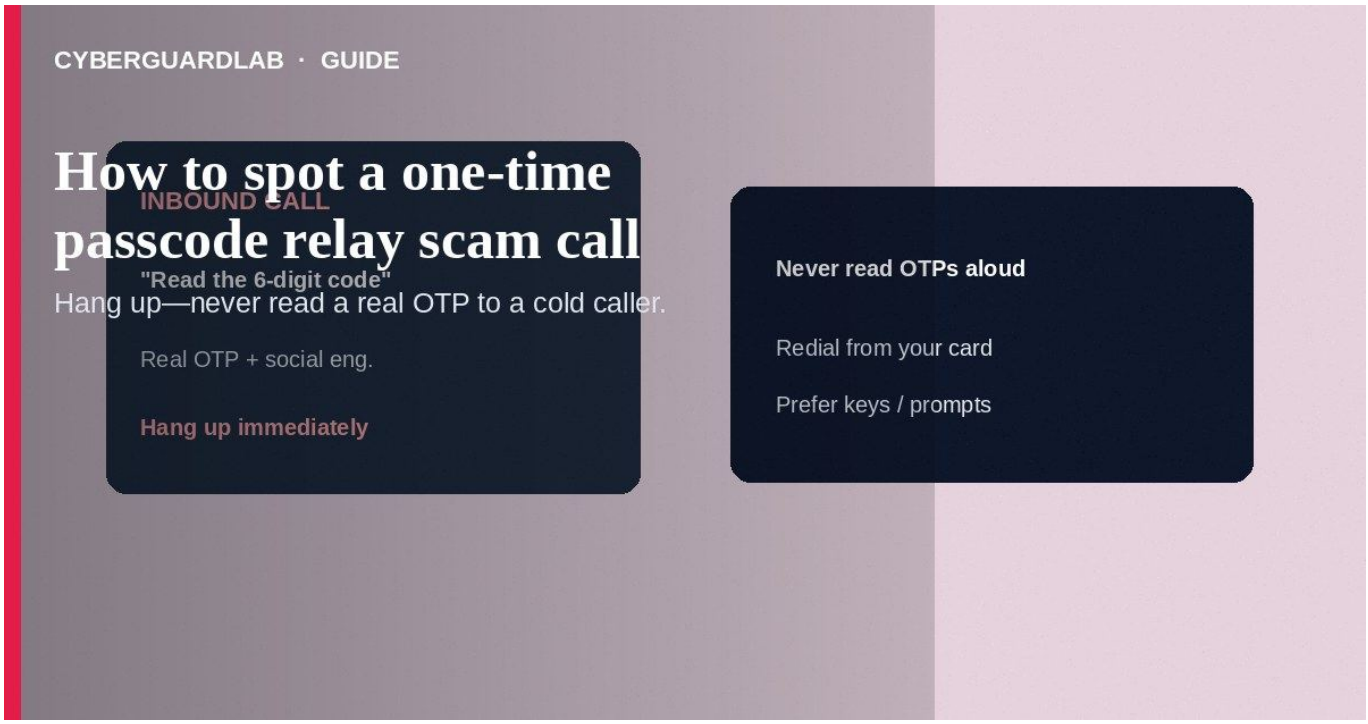


How to spot a one-time passcode relay scam call

https://cyberguardlab.com/blog/otp-relay-scam-call

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



An OTP relay scam call is when a live person (or AI voice) phones you, pretends to be your bank, Apple, Google, Microsoft, or "fraud department," and coaches you to read aloud a one-time passcode that just arrived by SMS or app-so they can finish a login or reset they already started. Hang up. Do not share the code. Call the number on your card or open the official app yourself. This guide is about voice/video relay of real codes-not a fake 2FA phishing text that mainly pushes a link, and not Google Prompt approval fatigue alone.

1. How OTP relay scam calls work

You get an unexpected call: "We see a transfer from your account-enter the code we just texted to cancel it." Or "Apple Security-your iCloud was locked; read the six digits on your screen." The code is often a real OTP from the service because the attacker already has your password or is mid-reset. Reading the digits completes their access. Some scripts ask you to install remote-support software so they can "see the code with you."

Unlike a fake 2FA text that tries to make you tap a phishing URL, OTP relay weaponizes a legitimate code plus social engineering on the phone.

Scammers invent a fake outgoing wire and claim reading the SMS "stops" it. Reading the code often authorizes their session. Teach household members: one-time codes are secrets, never cancel buttons, and banks will not ask for them on a cold call.

2. Red flags before you share a code

Cue | Likely legitimate | Likely scam

Who started contact | You called the number on your card or opened the official app | Cold call or callback after a spoofed "bank" SMS

What they ask | Never asks you to read an OTP aloud | "Confirm the code we sent" or "forward it to cancel"

Timing of OTP | Code arrives only after you start a login you know about | Code arrives during the call you did not start

Channel | In-app chat after you sign in yourself | Pressure to stay on the line while you dig for the SMS

Remote access | Banks and Apple do not need AnyDesk/TeamViewer for OTP | Install screen-share "so we can secure the account"

Threats | Calm steps inside the official app | Arrest, account wipe, or "minutes left" urgency

3. Safer habits (buy-nothing)

* Hang up. Do not argue or "just verify one digit."
* Do not read, forward, or type the OTP for anyone who contacted you first.
* If an SMS code arrived during the call, treat it as an active attack: open the real bank/Apple/Google app or bookmark and check recent security activity; change the password from a clean session if needed.

* Call your bank using the number on the back of your card-or use in-app secure message-not a number the caller gave you.
* Prefer authenticator apps, passkeys, or hardware security keys over SMS where available.
* For unexpected security texts without a call, see fake 2FA text.

4. If you already shared a code

* Assume that account may be taken over. Change the password immediately from another device if needed; sign out other sessions.
* Contact the bank or service through official channels; ask them to freeze transfers and review recent logins.
* Change the email password that recovers the account; turn on stronger 2FA.
* If remote-access software was installed, uninstall it, disconnect from the network if advised by the bank's fraud team, and scan the PC.
* Report at ReportFraud.ftc.gov; use IdentityTheft.gov if ID or account numbers were taken.
* Scan phones and PCs with a trusted tool such as Norton or Bitdefender. Keep one primary real-time antivirus-avoid stacking full suites. TotalAV, McAfee, and Avast are other on-site comparison options.

FAQ

Is OTP relay the same as a fake 2FA text?

No. Fake 2FA texts often push phishing links or spoofed alerts. OTP relay uses a live call (or chat) to harvest a real code that already arrived.

Can my bank ask for an OTP on an inbound call?

Treat inbound requests for codes as fraud. Real help starts from numbers or apps you open yourself.

What if the caller ID shows my bank's name?

Caller ID can be spoofed. Hang up and redial from the card or official site.

Does Google Prompt replace this risk completely?

Prompt/push approvals reduce SMS relay risk but still require you never approve a sign-in you did not start-see Google Prompt guide.

If you still want a paid suite

Avoiding how to spot a one-time passcode relay scam call does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* FTC: How to recognize phishing
* FTC: Imposter scams
* CISA: Multi-factor authentication
* IdentityTheft.gov
* FTC ReportFraud

Also read

* How to spot a fake two-factor authentication text
* How to turn on Google Prompt instead of SMS codes
* How to use a hardware security key for your main accounts
* How to set a carrier account PIN to stop SIM swap
* How to spot a fake Apple Support screen-sharing scam